WHAT IS CLAIMED IS:

1. A system for providing an enterprise-based security policy, the system comprising:

a central agent configured to retrieve a policy skin from a database and to transmit the policy skin to a host;

a data gathering engine configured to collect host data related to the host; and

a policy engine configured to execute the policy skin against the host data to determine security policy compliance.

2. The system of claim 1, further comprising a host agent configured to transmit the host data and compliance information to the central agent.

3. The system of claim 2, further comprising a scheduler configured to schedule when the data gathering engine collects the host data, when the policy engine executes the security policy and when the host agent transmits the host data and the compliance information to the central agent.

4. The system of claim 2, wherein the central agent is further configured to transmit the host data and the compliance information to the database for storage.

5. The system of claim 4, further comprising a report engine coupled to the database, the report engine configured to access the host data and the compliance information from the database and to generate a report based on the host data and the compliance

information.

6. The system of claim 1, wherein a central server includes the central agent, and the host includes the data gathering engine and the policy engine.

7. The system of claim 1, wherein the policy skin when retrieved from the database includes one or more policy strings, and the policy skin when executed includes the one or more policy strings translated into a general purpose language.

8. The system of claim 1, wherein the policy skin when executed is configured to be compatible with an operating system running on the host.

9. The system of claim 1, further comprising a remote access engine coupled to the database, the remote access engine configured to enable a third party to design, implement, monitor or maintain the policy skin.

10. The system of claim 1, further comprising a policy editor coupled to the database, the policy editor configured to enable a user to create the policy skin using policy strings.

11. The system of claim 1, wherein the host is a member of a group.

12. The system of claim 1, wherein the central agent is configured to retrieve a high security level policy skin from the database and to transmit the high security level policy

skin to the host in the event of a crisis or emergency.

13. A language stack for providing an enterprise-based security policy, the language stack comprising:

a policy strings layer configured to include policy strings;

a policy definition language layer configured to include a policy definition language;

a first translator configured to parse policy strings into the policy definition language;

a general purpose language layer configured to include a general purpose language; and

a second translator configured to parse the policy definition language into the general purpose language.

14. The language stack of claim 13, wherein the general purpose language comprises Python language.

15. The language stack of claim 13, further comprising a system definition layer configured to include run-time libraries and support services.

16. The language stack of claim 15, wherein an executable version of a policy skin includes one or more policy strings that have been translated into the general purpose language.

17. The language stack of claim 16, wherein the executable version of the policy skin is configured to call one or more run-time libraries or one or more support services from the system definition language when executed.

18. The language stack of claim 16, wherein the executable version of the policy skin is configured to be compatible with an operating system running on a host.

19. A method for providing an enterprise-based security policy, the method comprising:

receiving a policy skin from a central server;

collecting host data related to a host;

executing the policy skin against the host data to determine security policy compliance; and

transmitting the host data and policy compliance information to the central server.

20. The method of claim 19, wherein executing the policy skin comprises calling one or more run-time libraries or one or more support services.

21. The method of claim 19, wherein the policy skin when executed includes one or more policy strings that have been translated into a general purpose language.

22. The method of claim 21, wherein the policy skin when executed is configured to be

compatible with an operating system running on the host.

23. The method of claim 19, further comprising the step of creating the policy skin, the policy skin including one or more policy strings.

24. The method of claim 23, wherein a policy editor or a remote access engine is used to create the policy skin.

25. The method of claim 19, further comprising the steps of receiving the host data and compliance information and storing the host data and compliance information in a database.

26. The method of claim 25, wherein the database resides in the central server.

27. The method of claim 25, further comprising the steps of accessing the host data and compliance information from the database and generating a report based on the host data and compliance information.

28. A system for providing an enterprise-based security policy, the system comprising:

means for receiving a policy skin from a central server;

means for collecting host data related to a host;

means for executing the policy skin against the host data to determine security policy compliance; and

means for transmitting the host data and policy compliance information to the central server.

29. The system of claim 28, further comprising means for creating the policy skin, the policy skin including one or more policy strings.

30. The system of claim 28, further comprising means for receiving the host data and compliance information and means for storing the host data and compliance information in a database.

31. The system of claim 30, further comprising means for accessing the host data and compliance information from the database and means for generating a report based on the host data and compliance information.